

FORA FINANCIAL HOLDINGS, LLC

Plaintiff,

VS.

NEW YORK TRIBECA GROUP, LLC and JOHN
DOES 1-10,

Defendants.

-X

:

:

: Case No. _____

$$\vdots$$

:

:

:

•

•

•

•

:

$$-\lambda$$

DECLARATION OF KEVIN RUTHEN

I, Kevin Ruthen, of full age, hereby declare the following:

1. I am the Chief Technology Officer of Fora Financial Holdings, LLC (“Fora Financial”).
2. I make this declaration based upon personal knowledge and my review of business records maintained by Fora Financial.

Fora Financial's Efforts to Protect Its Trade Secrets and Confidential Information

3. Fora Financial expends significant time, resources, and money in protecting the confidentiality of its trade secrets, confidential, and proprietary information (the “Protected Information”), including electronically stored information.
4. Access to Fora Financial’s systems, including emails and shared drives, is password protected, subject to multi-factor authentication when supported and controlled by a central administrator.
5. Fora Financial enforces strong password policies (requiring the use of upper case letters, lower case letters, numbers, and symbols).

6. Fora Financial stores the Protected Information on a cloud storage system with a “zero trust” framework. This means that Fora Financial’s system requires all users, inside or outside the network, to be authenticated, authorized and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

7. Fora Financial deploys endpoint virus protection, as well as a multilayer defense that permits Fora Financial to monitor, detect and prevent detect threats to its systems.

8. Some Fora Financial employees access Fora Financial’s system remotely. Any such remote access to Fora Financial’s system occurs through Zscaler, a cloud security company.

9. Among other security measures, Zscaler prevents access to public websites and can prevent the downloading of data to a device’s local drives while working remotely.

10. Fora Financial’s employment agreements contain confidentiality provisions prohibiting employees from disclosing Fora Financial’s confidential information.

11. Fora Financial’s policy is that, upon termination, an employee’s access to all of Fora Financial’s systems is terminated immediately. Fora Financial uses a single sign-on (“SSO”) and multi-factor authentication security program called Okta, which controls an employee’s access to Fora Financial’s system. Therefore, when an employee is terminated, their Okta access is revoked and their access to Fora Financial’s systems is removed.

12. Employees are required to return any devices, documents and information in their possession on their last day of work for Fora Financial.

13. Fora Financial engages in wide scale penetration testing and vulnerability assessments in order to test its security measures and systems.

Investigation into the Misappropriation of Protected Information

14. It is my understanding that on or about September 7, 2022, Fora Financial received reports from independent sales organizations (“ISOs”) and brokers that certain customers who had submitted applications to Fora Financial for new and renewal financing were being solicited by agents of New York Tribeca Group, LLC (“Tribeca”).

15. The contents of these communications demonstrated to Fora Financial that Tribeca’s agents possessed Protected Information about Fora Financial’s customers and that Tribeca’s agents knew the merchant customers had applied for financing.

16. Around the same time, Fora Financial began receiving similar reports directly from customers that they also were receiving unwanted calls and text messages from Tribeca’s agents soliciting those customers to, among other things, seek financing from Tribeca.

17. Fora Financial’s communications with its customers and the relevant ISO’s and brokers demonstrated that Tribeca’s agents possessed Fora Financial’s Protected Information—including customers’ bank statements, personal contact information, business information (including tax identification numbers and the company’s revenue), and information about Fora Financial’s proposed financing, including the amount and length of the deal—and were using that Protected Information to solicit Fora Financial’s customers.

18. Fora Financial immediately began investigating if and how its Protected Information was being misappropriated.

19. On or around September 14, 2022, Fora Financial partnered with one of its brokers to begin planting “honeypot” application traps in its system to show that the information Tribeca possessed could have been obtained only from Fora Financial’s system and to try to determine the source of the theft of the Protected Information.

20. The “honeypot” application traps contained some real merchant information and some fake merchant information that was created and controlled by Fora Financial.

21. For instance, cell phone numbers owned by Fora Financial were listed as contact information for the names of real customers. Thus, when applications or the data on those applications were accessed and disclosed without authorization, the recipients of that pilfered data would, when attempting to contact the listed customers to solicit their business, instead contact employees of Fora Financial, who would document the interaction.

22. In other instances, Fora Financial created fake merchant names on the applications. Anyone who received this information as a “lead” could run a simple internet search to determine that the businesses Fora Financial created do not actually exist.

23. The “honeypot” application traps were then placed onto Fora Financial’s system.

24. Over the past few weeks, Fora Financial has been receiving phone calls and text messages from competitors soliciting customers for financing to the contact numbers placed on the “honeypot” application traps, including nearly 20 times by Tribeca’s agents.

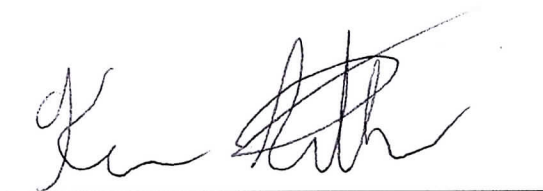
25. The data on the “honeypot” application traps was, and continues to be, misappropriated from Fora Financial’s system and used by those in possession of it to attempt to solicit Fora Financial’s customers.

26. Fora Financial tracked its interactions with competitors who contacted “honeypot” numbers to solicit Fora Financial’s customers.

27. Defendant Tribeca used honeypot information stolen from Fora Financial’s system over 20 times from September 15 through September 27.

I declare under penalties of perjury under the laws of the United States and New York that the foregoing is true and correct to the best of my knowledge.

Dated: October 6, 2022

A handwritten signature in black ink, appearing to read "Kevin Ruthen", written over a horizontal line.

Kevin Ruthen